

Allowable Subject Matter

1. Claims 1-11, 13-22, 24-30 and 33-34 are allowed.
2. The following is a statement of reasons for the indication of allowable subject matter: The present invention is directed to a prime calculating apparatus for calculating primes whose generation source can be identified, a prime verification apparatus for performing the identification, a key issuing system, a prime calculation method, a prime verification method and a computer program. The independent claims identify the unique features of having the prime calculating apparatus calculates multiplication value R by multiplying the management information corresponding to the prime to be generated by the random number, and calculates prime candidate N , according to $N = 2 \times \text{multiplication value } R + w) \times \text{prime } q + 1$, using $2 \times w \times \text{prime } q + 1 = \text{the verification value (mod the management information)}$. As a result, when the calculated prime candidate N is a prime, the generation source of the prime can be identified by judging whether $(\text{prime } N - \text{the verification value})$ is divisible by the management information. The prior arts of record fail to anticipate or render the above limitations obvious.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

3. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873.

Art Unit: 2438

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi T. Arani can be reached on 571-272-3787. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Minh Dieu Nguyen/

Primary Examiner, Art Unit 2438